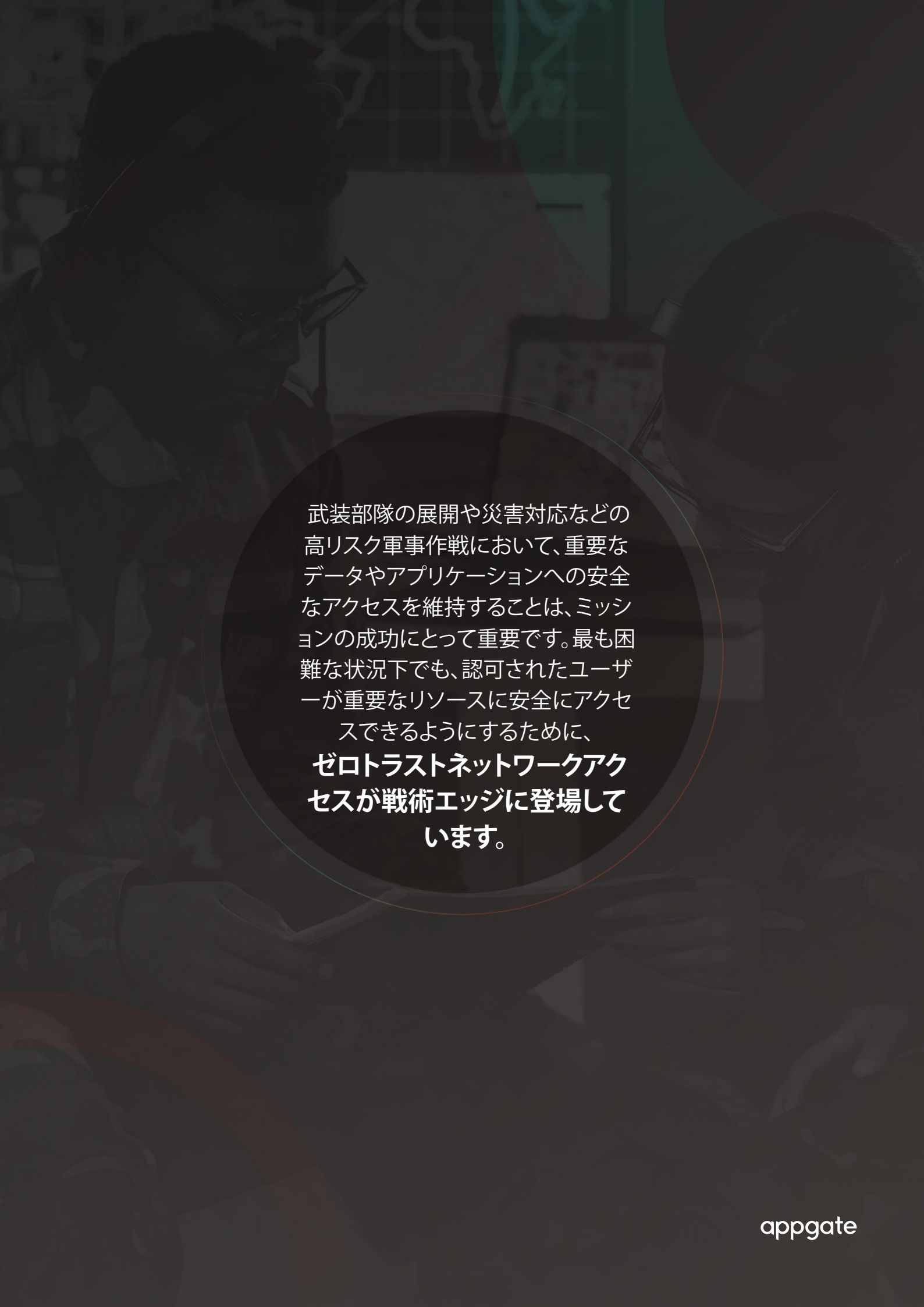
appgate

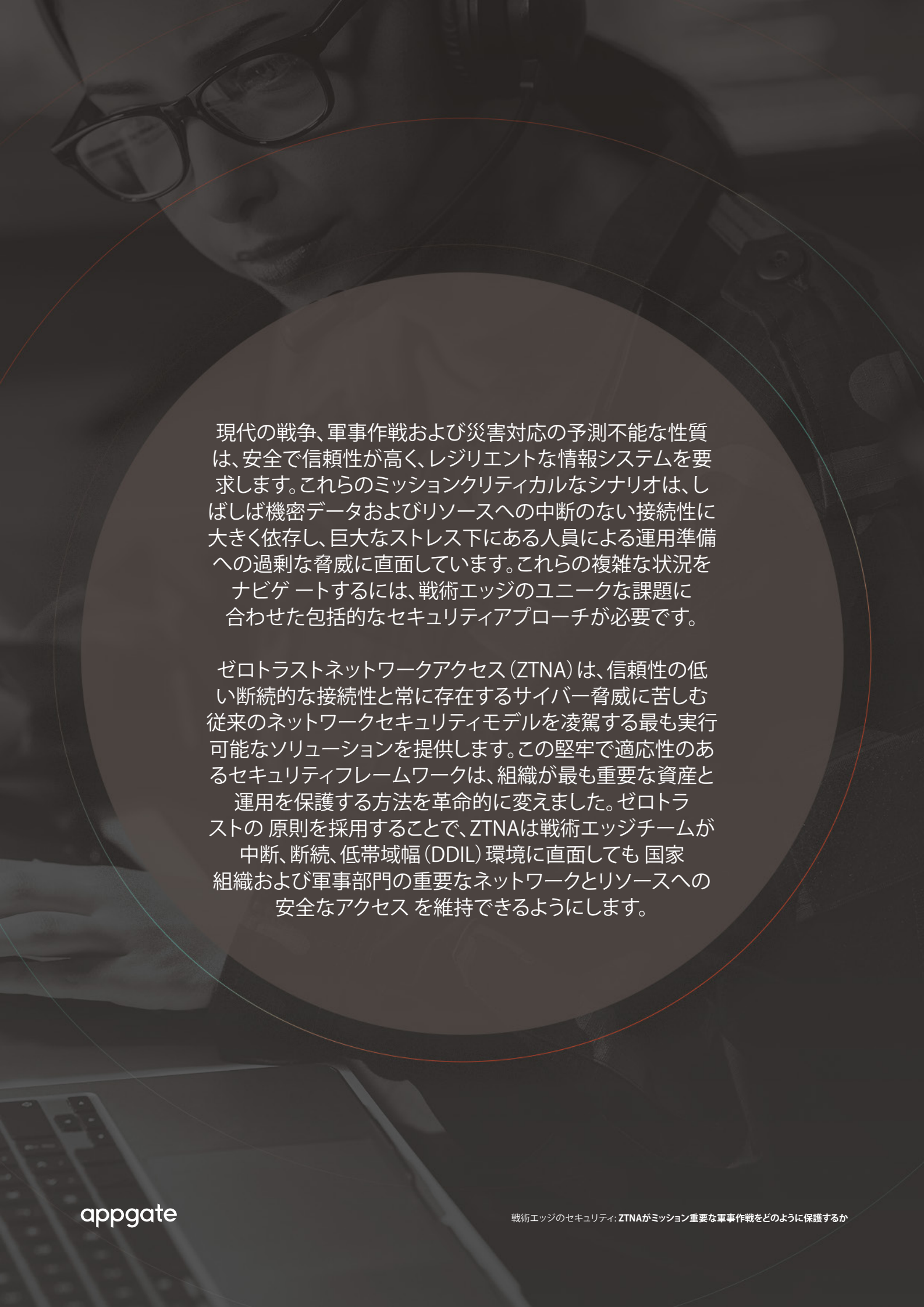
戦術エッジのセキュリティ: ZTNAがミッションクリティカルな軍事作戦をどのように保護するか



武装部隊の展開や災害対応などの高リスク軍事作戦において、重要なデータやアプリケーションへの安全なアクセスを維持することは、ミッションの成功にとって重要です。最も困難な状況下でも、認可されたユーザーが重要なリソースに安全にアクセスできるようにするために、**ゼロトラストネットワークアクセスが戦術エッジに登場しています。**

appgate

目次



現代の戦争、軍事作戦および災害対応の予測不能な性質は、安全で信頼性が高く、レジリエントな情報システムを要求します。これらのミッションクリティカルなシナリオは、しばしば機密データおよびリソースへの中断のない接続性に大きく依存し、巨大なストレス下にある人員による運用準備への過剰な脅威に直面しています。これらの複雑な状況をナビゲ ートするには、戦術エッジのユニークな課題に合わせた包括的なセキュリティアプローチが必要です。

ゼロトラストネットワークアクセス（ZTNA）は、信頼性の低い断続的な接続性と常に存在するサイバー脅威に苦しむ従来のネットワークセキュリティモデルを凌駕する最も実行可能なソリューションを提供します。この堅牢で適応性のあるセキュリティフレームワークは、組織が最も重要な資産と運用を保護する方法を革命的に変えました。ゼロトラストの 原則を採用することで、ZTNAは戦術エッジチームが中断、断続、低帯域幅（DDIL）環境に直面しても 国家組織および軍事部門の重要なネットワークとリソースへの安全なアクセス を維持できるようにします。

戦術エッジのサイバーセキュリティ課題の理解

戦術エッジ固有の時間に敏感な重要な決定は即時かつ重大な結果をもたらし、安全なアクセスを最優先事項にします。しかし、運用の最前線で急速に変化し進化する状況は、独自のセキュリティ課題を提示します。それらには以下が含まれます：

接続の中断：

戦術作戦は、インターネット接続および従来のネットワークインフラが信頼できないか存在しない、遠隔地、孤立した地域、または争点地域で行われる場合があります。これらのDDIL環境でミッション クリティカルなリソースへの安全なアクセスを維持することは常に課題です。

多様な通信モード：

戦術チームは、衛星通信、5G、Wi-Fiメッシュ、IP経由のラジオなど、さまざまな通信方法を活用する必要があるかもしれません。これらの多様な通信モードを統合し、安全にすることはミッションの成功に不可欠です。

レガシーシステムおよび運用技術：

戦術エッジには、重要な機能に使用される現代のITシステム、レガシー機器、および運用技術の混在が含まれることがよくあります。これらの異なるシステムを保護し統合することは困難な作業です。

高まるサイバー脅威：

戦術エッジは、サイバー敵対者が積極的にシステムを破壊または侵害しようとする高リスク環境です。サイバー脅威からミッション クリティカルなデータおよびリソースを保護することが最重要課題です。

モビリティと切断された操作：

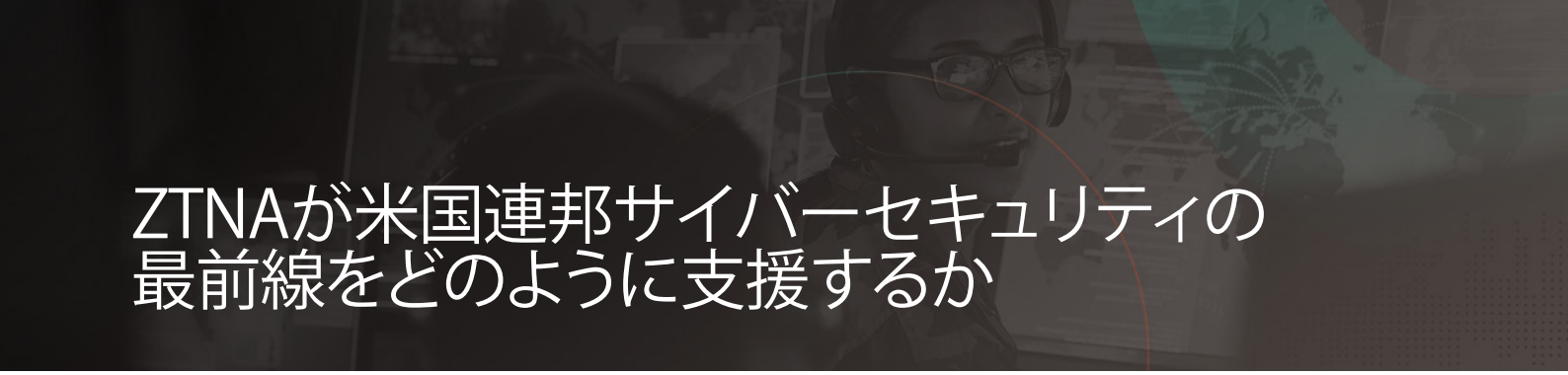
戦術チームはしばしば、ユーザーとデバイスが常に移動して高度に移動可能で切断された方法で操作する必要があります。この動態は、安全な接続と可視性を維持するための障害を引き起こす可能性があります。

軽微な遅延や脆弱性でもミッションの成功や人員の安全に重大な影響を与える可能性があるため、戦術エッジでは機敏で適応可能なセキュリティ対策が重要です。

制限されたコンピューティングパワーやストレージなどの限られたリソースは、効果を損なわない軽量なセキュリティソリューションを必要とします。しかし、VPNなどの従来のセキュリティソリューションは、戦術エッジでの不安定なネットワーク条件のような変動性に対処するのに不十分であることがよくあります。

加えて、VPNはユーザーとデバイスの急増をサポートするために迅速にスケールすることや、戦術エッジ操作を実行するために使用される多様なデバイスとプラットフォームに対応することができません。

VPNのような従来のセキュリティソリューションは、戦術エッジでの不安定なネットワーク条件のような変動性に対処するのに不十分であることがよくあります



ZTNAが米国連邦サイバーセキュリティの最前線をどのように支援するか

これらの独自の課題に対処するために、連邦機関はますますゼロトラストネットワークアクセスを選択肢として採用しています。ZTNAは、従来のネットワーク中心のセキュリティから、ユーザーのアイデンティティ、デバイスの状態、およびアプリケーションの動作などのコンテキスト要因に基づいてアクセスを検証する、ユーザー、リソース、およびデータ中心のアプローチに焦点を移す現代のセキュリティフレームワークです。ZTNAの核心原則である「決して信頼せず、常に確認する」は、すべてのユーザー、デバイス、およびアプリケーションを潜在的な脅威として扱い、厳格な検証プロセスの後にのみアクセスを許可することを意味します。

さらに、場所やネットワーク接続状態に関係なく、ユーザーとデバイスを継続的に認証および認可します。このアプローチは、信頼の境界が絶えず変動し、従来の境界ベースのセキュリティモデルが適応できない戦術エッジに特に適しています。ゼロトラストアクセスソリューションは、切断された操作を保護するためにいくつかの重要な原則を採用しています：

アイデンティティ、デバイス、データ中心：

ZTNAは強力なユーザーおよびデバイス認証を優先し、認可された人員のみが機密データおよびリソースにアクセスできるようにします。多要素認証および継続的認証がよく使用され、最高レベルのセキュリティを維持します。

最小特権の原則：

ZTNAは、ユーザーがタスクを遂行するために必要な最小レベルのアクセスをユーザーに付与します。これにより、資格情報が侵害された場合に攻撃者が引き起こす可能性のある損害を制限します。

継続的な監視と適応的なアクセス：

ZTNAは、ユーザー、デバイス、および環境要因を動的に評価して、リアルタイムのアクセス決定を行います。これにより、進化する状況に迅速に対応する適応的なアクセス制御が可能になり、特定の瞬間に認可されたユーザーのみが適切なレベルのアクセスを持つことが保証されます。

安全なマルチモード接続：

ZTNAは、衛星通信、5G、Wi-Fiメッシュ、IP経由のラジオなどのさまざまな通信モードと統合して、多様な戦術エッジ環境で安全なアクセスとデータ共有を提供できます。

安全なワークロード移行：

ZTNAは、戦術エッジと指揮センター間でコンテナ化されたワークロードおよびアプリケーションの安全な移行を可能にし、最も必要な場所にミッション クリティカルなリソースを迅速に展開できるようにします。

シームレスな切断された操作：

ネットワークの中断が発生した場合、ZTNAは戦術エッジのローカルリソースへの安全なアクセスを維持し、ユーザーが中断なく重要な機能を継続できるようにします。有効性を損なわないソリューションです。

ZTNAは、すべてのユーザー、デバイス、およびアプリケーションを潜在的な脅威として扱い、厳格な検証プロセスの後にのみアクセスを許可します。

Appgate SDP:
戦術エッジ操作向けの差別化されたZTNA

業界をリードするZTNAソリューションであるAppgate SDPは、戦術エッジの独自のセキュリティ課題に対処する際に優れており、連邦機関および軍事部門のユースケースに最適です。
具体的には、Appgate SDP ZTNA は、米国国防総省（DoD）の多くのサービス部門（宇宙軍、海兵隊、海軍、空軍を含む）で認定され、完全に運用可能です。また、DoDインパクトレベル6での運用許可を取得しており、米軍司令部による厳格なペネトレーションテストを受け、コモンクライテリア認証を取得した唯一のZTNAソリューションです。

さらに、Appgate SDP ZTNA は、重要なリソースへの安全で信頼性の高いアクセスを確保するための差別化された機能を提供します：

ダイレクトルーティングアーキテクチャ：

トラフィックを中央クラウドホスティングサービスまたはプロキシを介してルーティングする必要がなく、インターネット接続が利用できない場合でもリソースへの低遅延アクセスを保証します。

シングルパケット認証（SPA）：

ネットワークエッジを隠蔽し、敵が保護されたリソースを特定して攻撃することを困難にします。

相互TLS（mTLS）技術：

通信のセキュリティを強化し、中間者攻撃やセッションハイジャックのようなサイバー脅威を軽減します。

ワークロード移行：

アプリケーションを中央指令と戦術エッジの間でシームレスに移行でき、最適なパフォーマンスと可用性を保証します。

ダイレクトルーティングZTNAとは？

ダイレクトルーティングZTNAアーキテクチャは、企業内の独自のプライベートアプリケーションとネットワークインフラストラクチャに対応するための目的構築された柔軟なアプローチを提供します。このモデルは、データがネットワークを通過する方法を完全に制御し、どこにでも配置されたハイブリッドインフラストラクチャ全体からのユーザーからリソースへの、リソースからリソースへの接続に安全なアクセスを提供します。

主な利点は、ダイレクトルーティングアーキテクチャのスケーラビリティとパフォーマンスであり、企業は最適なネットワークパフォーマンスを維持しながらビジネスを拡大することができます。ダイレクトルーティングZTNAに関連する価格モデルは透明で、理解しやすく、隠れた料金がなく、企業に予測可能で管理しやすいコスト構造を提供します。

ゼロトラストネットワークアクセス（ZTNA）は、米国連邦組織が切断された環境や戦術的エッジ環境での操作をどのように保護するかを革命的に変えています。現代の戦争、軍事作戦、危機対応の進化する状況は、戦術エッジのユニークな課題に対する適応可能なセキュリティソリューションを要求しています。

操作環境が進化するにつれ、ZTNAを採用する米国連邦機関は、資産を保護し、ミッションの成功を確保し、新たに発生するサイバー脅威に対する戦略的優位性を維持する準備が整います。

Appgate SDP、ZTNAは、ダイレクトルーティングアーキテクチャを使用してネットワーク防御を革命化し、最も過酷な環境でのミッションクリティカルな操作を保護します。

Appgate SDP、ZTNAが切断された戦術的エッジ操作をどのように保護するかについて詳しく知りたいですか？
今すぐZTNAテーブルトークのリプレイを視聴してください。

Appgateは、企業の最も貴重な資産とアプリケーションを保護します。Appgateは、ゼロトラストネットワークアクセス（ZTNA）とオンライン詐欺保護の市場リーダーです。Appgateの製品には、ユニバーサルZTNA用のAppgate　SDPと360詐欺保護が含まれます。Appgateのサービスには、脅威アドバイザリー分析とZTNAの実装が含まれます。Appgateは、世界中の企業と政府機関を保護します。詳細は appgate.com をご覧ください。

appgate